UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of)
Storage unit 2205 located at 12714 S. La Cienega Blvd., Hawthorne, California 90250)
) Case No. **2:24-MJ-00557**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Distribution of Controlled Substances
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 922(a)(1)(A)	Engaging in business of dealing firearms without license
18 U.S.C. § 933	Trafficking in firearms

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of_____days (*give exact ending date if more than 30 days*:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Emma Largerie

Applicant's signature

Emma Largerie, ATF Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.
Date: _____

Judge's signature

City and state: Los Angeles, CA

Hon. Charles Eick, U.S. Magistrate Judge

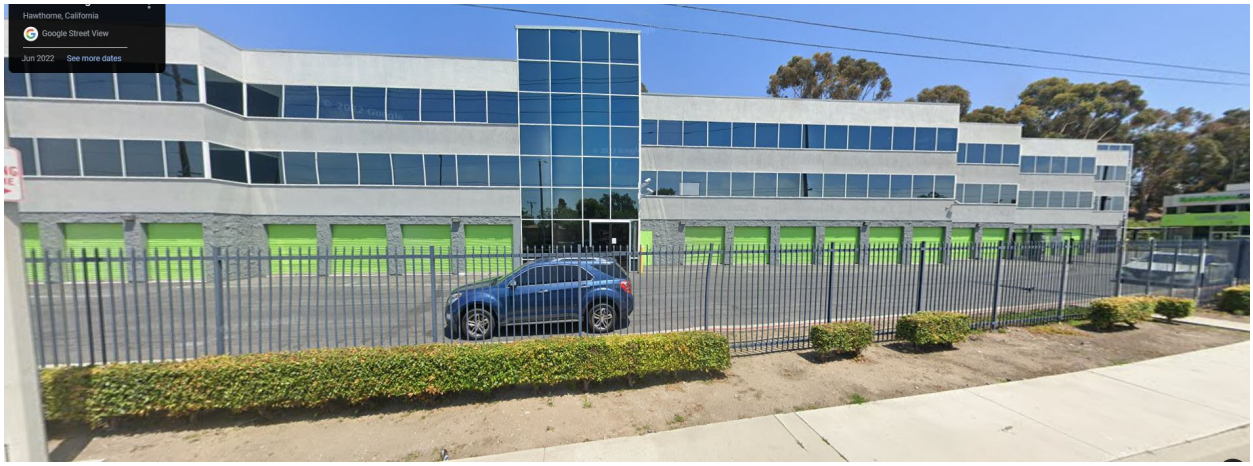
Printed name and title

AUSA: K. Afia Bondero (x2435)

ATTACHMENT A

PREMISES TO BE SEARCHED

SUBJECT PREMISES 3 is storage unit 2205 at 12714 S. La Cienega Blvd., Hawthorne, California 90250. SUBJECT PREMISES 3, as depicted in the photograph, is a storage unit inside an Extra Space Storage facility.



ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 922(a)(1)(A) (engaging in the business of dealing firearms without a license), 18 U.S.C. § 933 (trafficking in firearms), 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances), and 21 U.S.C. § 841(a)(1) (distribution of a controlled substance) (the "Subject Offenses"), namely:

a. Any controlled substance, controlled substance analogue, or listed chemical;

b. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;

c. Firearms and ammunition;

d. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;

e. United States currency over $1,000 or bearer instruments worth over $1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first $1,000), and data, records,

documents, or information (including electronic mail, messages over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or transferring money over $1,000, such as bank account records, cryptocurrency records and accounts;

f. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances or firearms, or drug or firearms customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs, guns, or ammunition, were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

g. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

h. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written

communications sent to or received from any of the digital devices and which relate to the above-named violations;

i. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

j. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs, firearms, or ammunition;

k. Contents of any calendar or date book;

l. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

m. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

n. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

4. In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or

seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending),

including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress SIERRA's thumb- and/or fingers onto the fingerprint sensor of the digital device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of SIERRA's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Emma Largerie, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF") and have been a federal law enforcement officer since March 2023. I am currently assigned to the Los Angeles Field Division, where I participate in investigations involving, among other federal offenses, prohibited persons possessing firearms, persons trafficking firearms and controlled substances, and persons possessing illegal firearms. I have also participated in investigations focusing on gang activity and transnational organizations. I have participated in multiple ATF operations and assisted local police investigating violations of firearms and narcotics laws. I have also received both basic and specialized training about violations of federal firearm laws and the methods used to investigate those violations.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a search warrant for Extra Space Storage, Unit #2205, located at 12714 S. La Cienega Blvd., Hawthorne, California 90250 ("SUBJECT PREMISES 3") described in Attachment A, for the items to be seized described in Attachment B, which are the evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 922(a)(1)(A) (engaging in the business of dealing firearms without a license), 18 U.S.C. § 933 (trafficking in

firearms), 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances), and 21 U.S.C. § 841(a)(1) (distribution of controlled substances) (the "Subject Offenses").

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, and all dates and times are on or about those indicated.

III. SUMMARY OF PROBABLE CAUSE

4. On January 29, 2024, the Honorable Charles Eick, United States Magistrate Judge for the Central District of California, signed a complaint and issued federal search warrants authorizing the arrest and search of GEOVANY DANIEL SIERRA, his residence at 620 Illinois Ct. Apt 17, El Segundo, California 90245 ("Subject Premises 1"), his previous storage unit C231 at 1910 Hughes Way, El Segundo, California 90245 ("Subject Premises 2"), and two vehicles he drove, including any digital devices he possessed, for evidence related to the Subject Offenses. See 24-MJ-00454-DUTY, 24-MJ-00456-00458-DUTY, 24-MJ-00460-00461-DUTY. The application filed in support of the January 29 warrant for SIERRA's prior storage unit (i.e., Subject Premises 2), including the affidavit filed in support

(24-MJ-00457), is attached hereto as **Exhibit 1** and incorporated herein by reference.

5. After obtaining the January 29 Complaint and Warrants, federal agents learned SIERRA had cleared out his previous storage unit (Subject Premises 2) and rented a new storage unit at an Extra Space Storage facility, SUBJECT PREMISES 3. Between January 28 and January 29, 2024, an ATF undercover agent ("UC-2") and SIERRA exchanged multiple text messages to confirm the details of the firearms transaction they had been discussing over the course of the last several weeks. UC-2 and SIERRA agreed to meet at a location in Hawthorne, California on February 1, located less than a mile away from the location of SUBJECT PREMISES 3.

IV. STATEMENT OF PROBABLE CAUSE

6. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. SIERRA Dealt Firearms and Distributed Controlled Substances

7. As detailed in **Exhibit 1**, between September 2023 and December 2023, two ATF UCs purchased nine firearms, one machine gun conversion device, and approximately 1,500 fentanyl pills on five separate occasions from SIERRA. On two of those occasions, SIERRA sold the firearms in the close proximity of his previous Public Storage, storage unit C231 located at 1910 Hughes Way in El Segundo, California. Surveillance footage from the Public

Storage facility is consistent with SIERRA removing firearms from his unit prior to the controlled purchases.

8. SIERRA did not have a license to sell firearms.

B. SIERRA Obtains A New Storage Unit

9. On January 29, 2024, after obtaining a search warrant for SIERRA's Public Storage unit C231 (Subject Premises 2, see 24-MJ-00454), I learned that SIERRA no longer leased storage unit C231 from Public Storage.

10. Based on my conversation with the UC-2, who remains in contact with SIERRA, between January 28 and January 29, 2024, UC-2 engaged in recorded cell phone communication with SIERRA. UC-2 and SIERRA exchanged multiple text messages in order to confirm the details of the firearms transaction they had been discussing over the course of the previous several weeks.

11. On January 28, 2024, UC-2 texted SIERRA that UC-2 would be ready to conduct the transaction on Thursday, February 1, 2024. SIERRA agreed.

12. On January 29, 2024, UC-2 and SIERRA agreed to meet in or around Hawthorne, CA. While discussing a meet location, the following text messages were exchanged between UC-2 and SIERRA (with incoming referencing text messages received by UC-2 and outgoing referencing text messages sent by UC-2):

Date	Time	Direction	Content
2024/01/29	05:57:39 PM PST	Incoming	I got a new storage spot
2024/01/29	05:57:48 PM PST	Incoming	So ima park somewhere around there
2024/01/29	05:58:15 PM PST	Incoming	Then have u pick me up and I'll bring everything out, I got some black containers so you can't see them

2024/01/29	05:58:54 PM PST	Incoming	2525 E El Segundo Blvd El Segundo, CA 90245 United States
2024/01/29	05:58:55 PM PST	Outgoing	Where's the storage unit?
2024/01/29	05:59:03 PM PST	Incoming	Ima prolly just leave my car there
2024/01/29	05:59:10 PM PST	Incoming	It's right down the street from that spot
2024/01/29	05:59:41 PM PST	Incoming	This one has a lot of cameras tho so they can see shit going on that's why I rather have u pick me up and I grab the Shit rq

13. An internet search revealed a retail store with a parking lot was located at the address SIERRA sent UC-2. A further search of the area revealed Extra Space Storage Facility was located less than a mile away at 12714 S. La Cienega Blvd Hawthorne, California.

14. On January 30, 2024, in response to a legal process served on Extra Space Storage, I spoke with an individual who identified himself as the manager of the Extra Space Storage Facility located at 12714 S. La Cienega Blvd., Hawthorne, California. He verbally confirmed from reading a business record that SIERRA became the lessee of Unit #2205 (i.e., SUBJECT PREMISES 3) beginning on January 23, 2024.[1]

[1] Later that day, SIERRA stated to UC-2 per a recorded conversation that SIERRA moved the firearms from the newly acquired Extra Space Storage Unit 2205. SIERRA stated to UC-2 that the location had been compromised and that SIERRA moved some of the firearms to an associated residence. In further recorded conversations between UC-2 and SIERRA. UC-2 asked SIERRA for clarification about the compromised storage unit. SIERRA replied that SIERRA's parents accused SIERRA of selling narcotics. SIERRA then decided to move all contraband to an unknown location.

However, per the conversation with the onsite manager at Extra Space Storage, the spontaneous comment was made that SIERRA was up to date with the monthly payment. While making the spontaneous comment, the onsite manager was checking the Extra

(footnote cont'd on next page)

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

15. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, and in their residences.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This

---

Space Storage database. Given the short timing and that I am unable to verify the veracity of SIERRA's statements claiming to have emptied SUBJECT PREMISES 3, I believe there is probable cause to believe that evidence of the SUBJECT OFFENSES is still present in SUBJECT PREMISES 3.

includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residence. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residence, including in the form of calendar entries and location data.

e. Drug traffickers often use vehicles to transport their narcotics and may keep stashes of narcotics in their vehicles in the event of an unexpected opportunity to sell narcotics arises.

f. Drug traffickers often maintain on hand large amounts of United States currency in order to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence or in safes. They also often keep other items related to their drug trafficking activities at their residence, such as digital

scales, packaging materials, and proceeds of drug trafficking. These items are often small enough to be easily hidden and thus may be kept at a drug trafficker's residence even if the drug trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

VI. TRAINING AND EXPERIENCE ON FIREARMS OFFENSES

16. From my training, personal experience, and the collective experiences related to me by other law enforcement officers who conduct who conduct firearms investigations, I am aware of the following:

a. Persons who possess, purchase, or sell firearms generally maintain records of their firearm transactions as items of value and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such in their digital devices. It has been my experience that prohibited individuals who own firearms illegally will keep the contact information of the individual who is supplying firearms to prohibited individuals or other

individuals involved in criminal activities for future purchases or referrals. Such information is also kept on digital devices.

b. Many people also keep mementos of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their digital devices. These photographs and recordings are often shared via social media, text messages, and over text messaging applications.

c. Those who illegally possess firearms often sell their firearms and purchase firearms. Correspondence between persons buying and selling firearms often occurs over phone calls, e-mail, text message, and social media message to and from smartphones, laptops, or other digital devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price. In my experience, individuals who engage in street sales of firearms frequently use phone calls, e-mail, and text messages to communicate with each other regarding firearms that the sell or offer for sale. In addition, it is common for individuals engaging in the unlawful sale of firearms to have photographs of firearms they or other individuals working with them possess on their cellular phones and other digital devices as they frequently send these photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms.

d. Individuals engaged in the illegal purchase or sale of firearms and other contraband often use multiple digital devices.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[2]

17. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

1. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

2. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

[2] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

3. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

4. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

18. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

19. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a

device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

20. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress **SIERRA**'s thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of **SIERRA**'s face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

21. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

//

//

//

//

//

VIII. CONCLUSION

22. For all the reasons described above, there is probable cause that the items listed in Attachment B, which constitute evidence, fruits and instrumentalities of the Subject Offenses, will be found in a search of SUBJECT PREMISES 3, as described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ____ day of January, 2024.

_____

THE HONORABLE CHARLES EICK
UNITED STATES MAGISTRATE JUDGE

EXHIBIT 1

UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
1/29/2024
CENTRAL DISTRICT OF CALIFORNIA
BY: DEPUTY

In the Matter of the Search of)
Storage unit C231 located at 1910 Hughes Way, El Segundo, California 90245)
) Case No. 2:24-mj-00457

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-2

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Distribution of Controlled Substances
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 922(a)(1)(A)	Engaging in business of dealing firearms without license
18 U.S.C. § 933	Trafficking in firearms

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Emma Largerie
Applicant's signature

Emma Largerie, ATF Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.
Date: 1/29/24

Judge's signature

City and state: Los Angeles, CA

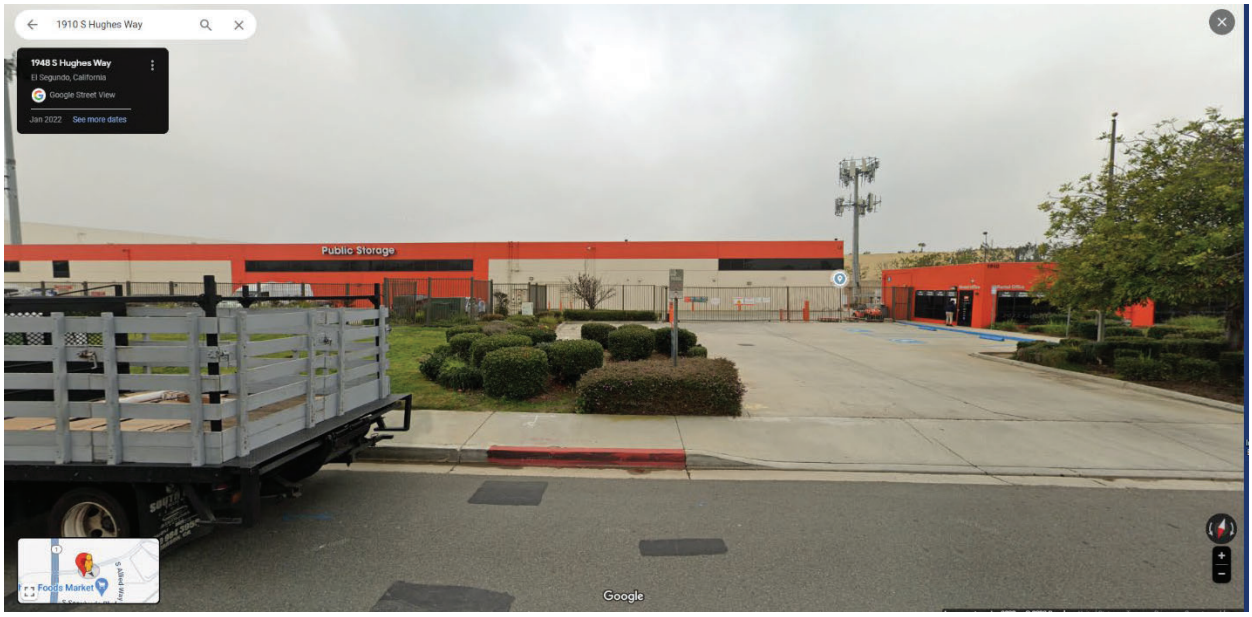
Hon. Charles Eick, U.S. Magistrate Judge
Printed name and title

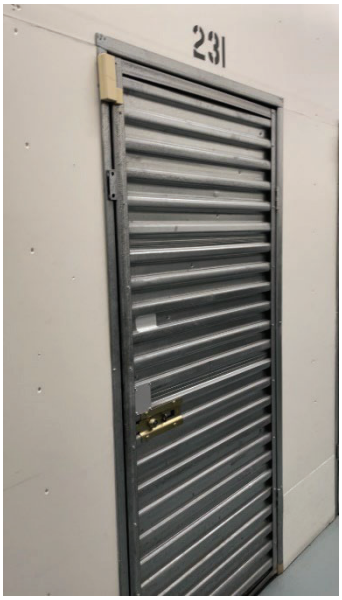
AUSA: K. Afia Bondero (x2435)

ATTACHMENT A-2

PREMISES TO BE SEARCHED

SUBJECT PREMISES 2 is storage unit C231 at 1910 Hughes Way, El Segundo, CA 90245. **SUBJECT PREMISES 2**, as depicted in the photograph below, is a storage unit inside a Public Storage facility.





ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 922(a)(1)(A) (engaging in the business of dealing firearms without a license), 18 U.S.C. § 933 (trafficking in firearms), 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances), and 21 U.S.C. § 841(a)(1) (distribution of a controlled substance) (the "Subject Offenses"), namely:

a. Any controlled substance, controlled substance analogue, or listed chemical;

b. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;

c. Firearms and ammunition;

d. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;

e. United States currency over $1,000 or bearer instruments worth over $1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first $1,000), and data, records,

documents, or information (including electronic mail, messages over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or transferring money over $1,000, such as bank account records, cryptocurrency records and accounts;

f. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances or firearms, or drug or firearms customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs, guns, or ammunition, were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

g. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

h. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written

communications sent to or received from any of the digital devices and which relate to the above-named violations;

i. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

j. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs, firearms, or ammunition;

k. Contents of any calendar or date book;

l. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

m. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

n. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

4. In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or

seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending),

including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress SIERRA's thumb- and/or fingers onto the fingerprint sensor of the digital device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of SIERRA's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Emma Largerie, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF") and have been a federal law enforcement officer since March 2023. I am currently assigned to the Los Angeles Field Division, where I participate in investigations involving, among other federal offenses, prohibited persons possessing firearms, persons trafficking firearms and controlled substances, and persons possessing illegal firearms. I have also participated in investigations focusing on gang activity and transnational organizations. I have participated in multiple ATF operations and assisted local police investigating violations of firearms and narcotics laws. I have also received both basic and specialized training about violations of federal firearm laws and the methods used to investigate those violations.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a criminal complaint and arrest warrant against GEOVANY DANIEL SIERRA ("SIERRA") for violations of 21 U.S.C. § 841(a)(1), (b)(1)(B): Distribution of a Controlled Substance.

3. This affidavit is also made in support of an application for warrants to search 620 Illinois Ct. Apt 17, El Segundo, California 90245 ("SUBJECT PREMISES 1") as described more fully in Attachment A-1, storage unit C231 located at 1910

Hughes Way, El Segundo, California 90245 ("SUBJECT PREMISES 2") as described more fully in Attachment A-2, a blue Toyota minivan bearing California license plate 5PTU385 ("SUBJECT VEHICLE 1") as described more fully in Attachment A-3, a gold Nissan minivan bearing California license plate 4FJU973 ("SUBJECT VEHICLE 2") as described more fully in Attachment A-4, and the person of SIERRA, as described more fully in Attachment A-5, for the items to be seized described in Attachment B, which are the evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 922(a)(1)(A) (engaging in the business of dealing firearms without a license), 18 U.S.C. § 933 (trafficking in firearms), 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances), and 21 U.S.C. § 841(a)(1) (distribution of controlled substances) (the "Subject Offenses"). Attachments A-1, A-2, A-3, A-4, A-5, and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrants, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. SUMMARY OF PROBABLE CAUSE

5. As discussed below, between September 2023 and December 2023, undercover ATF Special Agents ("UCs") purchased approximately nine firearms, one machine gun conversion device, and approximately 1,500 fentanyl pills from SIERRA. On October 19, 2023, in a recorded transaction, SIERRA sold approximately 500 pills with a net weight of 53.4 grams that contained fentanyl to a confidential informant working with the ATF. **SIERRA** does not have a federal firearms license that would allow him to engage in the business of dealing in firearms.

IV. STATEMENT OF PROBABLE CAUSE

6. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. On September 28, 2023, SIERRA Sells UC-1 Two Firearms

7. Based on my conversations with a confidential informant[1] (the "CI"), I am aware that original contact between the CI and **SIERRA** began in approximately April 2023. On September 15, 2023, the CI, working at the ATF's direction and under its supervision, informed me that a Telegram account, named @dannypu61, which the CI informed ATF was **SIERRA**'s account, had messaged him/her about prescription drugs available

[1] In early September 2023, the subject of a Los Angeles Police Department narcotics investigation voluntarily became an ATF CI. The CI has not yet been charged for the narcotics trafficking conduct. The CI has a felony conviction of arson of property. To date, ATF has paid the CI $1,000 to assist with rent and monthly bills. As set forth below, agents have taken steps to corroborate information provided by the CI and have found the CI to be reliable and credible.

for purchase.[2] The CI asked **SIERRA** if the firearms that were previously offered for sale in June 2023 were still available for purchase. **SIERRA** agreed and sent the CI photographs of two firearms.

8. On September 20, 2023, **SIERRA** contacted the CI and sent a different photograph of two firearms for sale. The CI offered **SIERRA** $850 per firearm or $1,500 for both. **SIERRA** agreed to sell both firearms for $1,500. The CI informed me that through previous contact he/she had met with **SIERRA** at two separate locations: (1) storage unit C231 located at a Public Storage facility at 1910 Hughes Way, El Segundo, California 90245 (i.e., **SUBJECT PREMISES 2**), and (2) near a park on E. Palm Ave in El Segundo, California.

9. On September 28, 2023, after being introduced by the CI to SIERRA as a purported firearms purchaser, an undercover ATF agent ("UC-1") purchased two firearms from **SIERRA** at a parking lot dictated by SIERRA across the street from the Public Storage facility where **SUBJECT PREMISES 2** is located. I have reviewed recording device footage and the report from this event. Based on my review of the recording device footage and conversations with UC-1, I know the following:

a. **SIERRA** entered UC-1's vehicle with a bag. While inside UC-1's vehicle, **SIERRA** opened the bag and removed a ziplock bag containing a Taurus, model G2C, 9mm pistol bearing serial number ADE390310 with an inserted magazine and a box of

[2] Messages between the CI and SIERRA from early September 2023 onward were preserved and I or other agents have reviewed these messages discussed herein.

9mm Winchester ammunition. **SIERRA** then removed a second ziplock bag containing a Smith & Wesson, model M&P 40 shield, .40 caliber pistol bearing serial number JFL0921 with a magazine inserted and an extra magazine. He sold the firearms and magazines to UC-1 for $1,500. **SIERRA** also said that if UC-1 wanted privately manufactured firearms ("ghost guns"), his source charges approximately $900 because they are untraceable. **SIERRA** told UC-1 that the firearms are transported from Texas.

b. **SIERRA** exited UC-1's vehicle and entered the driver's side of a blue Toyota minivan bearing California license plate 5PTU385 ("**SUBJECT VEHCLE 1**") to leave the site.

10. Following the transaction, based on my review of law enforcement databases, a police report, and California Department of Motor Vehicles ("DMV") records, I learned that **SUBJECT VEHICLE 1** was registered to Claudia M. Herrera, with an address of 620 Illinois Ct. Apt 17, in El Segundo, California 90245 (i.e., **SUBJECT PREMISES 1**). **SIERRA's** listed address on his California driver's license is also **SUBJECT PREMISES 1**. In addition, according to an El Segundo Police Department report dated October 15, 2023, **SIERRA** informed the police that **SUBJECT PREMISES 1** was his place of residence.

11. Based on law enforcement reports and discussing with UC-1, I am aware that after completing the deal, UC-1 contacted **SIERRA**, via the Telegram application under the username, @dannypu61. **SIERRA** replied, informing UC-1 that he had found other firearms for sale and proceeded to send UC-1 a photograph of the firearms.

12. Following the transaction, agents compared **SIERRA's** DMV photograph with the individual in the recorded footage from the September 28, 2023, purchase, confirming the individual in the video as GEOVANY DANIEL **SIERRA**, date of birth 02/28/2004, with California Driver's License Number Y6304118. SIERRA's California Department of Motor Vehicle records list him as standing 5'10" tall with black hair and brown eyes.

B. On October 5, 2023, SIERRA Sells UC-1 1,000 Fentanyl Pills

13. Based on my review of messages between UC-1 and **SIERRA**, and conversations with UC-1, I am aware that between September 28 and October 5, 2023, UC-1 and **SIERRA** had consistent conversations about the sale of firearms and narcotics via the Telegram application. On September 28, 2023, **SIERRA** asked UC-1 the amount of methamphetamine he/she wanted to purchase. UC-1 said approximately two ounces. **SIERRA** then offered to sell UC-1 1,000 fentanyl pills for $1,100.

14. On October 5, 2023, UC-1 purchased one thousand fentanyl pills from **SIERRA**. I have reviewed recording device footage and the report from this event and had a conversation with UC-1, and I am aware of the following:

a. Based on my review, I know that prior to UC-1 arriving at the meetup location, surveillance units saw **SIERRA** bend over, pick up an object from behind a nearby bush, and then exit onto E. Palm Avenue from the Illinois Court apartments located in El Segundo, California. **SUBJECT PREMISES 1** is an apartment within the Illinois Court apartments, and the

direction that **SIERRA** exited the apartment complex from was consistent with where **SUBJECT PREMISES 1** is located. **SIERRA** then stood on the sidewalk holding a small black bag while operating what appeared to be the cellular phone associated to the number 310-978-7198 (the "Subject Telephone") because he interacted with the device at the same time UC-1 was sending him messages. As discussed below, **SIERRA** later confirmed he was using the Subject Telephone because he provided that number to a second undercover ATF agent ("UC-2").

15. Shortly thereafter, **SIERRA** was observed walking up to the driver's side of UC-1's vehicle. **SIERRA** handed UC-1 a black plastic bag through the driver's side window of UC-1's vehicle. **SIERRA** entered the front passenger seat of UC-1's vehicle. UC-1 opened the black plastic bag and saw four bottles of generic Xanax pills and a white paper bag containing a clear plastic bag containing approximately 1,000 fentanyl pills, all of which **SIERRA** sold to UC-1 for $1,700. Later laboratory testing showed there to be 1,005 pills with a net weight of 105.1 grams containing fentanyl.

16. During the recorded transaction, **SIERRA** confirmed that the two firearms purchased by UC-1 on September 28, 2023, were transported from Texas. **SIERRA** stated that the source of the firearms from Texas would be acquiring more for sale.

C. On October 19, 2023, SIERRA Sells UC-1 Five Hundred Fentanyl Pills and was Given Approximately Two Grams of Methamphetamine for Free

17. Based on my review of messages between UC-1 and **SIERRA**, and conversations with UC-1, I am aware that between

October 6 and October 19, 2023, UC-1 and **SIERRA** had consistent conversations about the sale of firearms and narcotics via the Telegram application. Specifically, on October 17, UC-1 asked **SIERRA** if he had more fentanyl pills for sale. **SIERRA** asked UC-1 approximately how many fentanyl pills he/she wanted to purchase. UC-1 said 1,000 fentanyl pills. On October 18, **SIERRA** confirmed the narcotics were available for purchase by UC-1. On October 19, prior to the controlled purchase, **SIERRA** sent UC-1 a picture of approximately 500 fentanyl pills and approximately two grams of methamphetamine.

18. On October 19, 2023, UC-1 purchased five hundred fentanyl pills, which later lab testing determined had a net weight of 53.4 grams and contained fentanyl. I have reviewed recording device footage, the report from this event, and had a conversation with UC-1, and am aware of the following:

a. Prior to the UC arriving, surveillance units observed **SIERRA** drive into the parking lot of 101 S. Sepulveda Boulevard, El Segundo, California in a gold Nissan minivan bearing California license plate 4FJU973 ("**SUBJECT VEHICLE 2**").

b. During this meeting, **SIERRA** delivered to UC-1 approximately 500 pills in exchange for $500.

c. During this meeting, **SIERRA** also handed UC-1 two gross grams of suspected methamphetamine as a free sample. **SIERRA** stated to UC-1 that if he/she wanted to purchase more methamphetamine from the source of the sample he/she should inform **SIERRA** and he would facilitate the sale.

19. Following the transaction, based on my review of law enforcement databases, I learned that **SUBJECT VEHICLE 2** was registered to Amilcar Jeovany Sierra, with an address of **SUBJECT PREMISES 1.**

D. On November 8, 2023, SIERRA Sells UC-2 Six Firearms, A Machine Gun Conversion Device, and Gave UC-2 .98 Grams of Methamphetamine for Free

20. Based on my review of messages between UC-1 and **SIERRA**, and conversations with UC-1, between October 20 and November 8, 2023, I know that UC-1 and **SIERRA** had continuing conversations about the sale of firearms and narcotics via the Telegram application on the Subject Telephone. On October 25, **SIERRA** contacted UC-1, informing UC-1 that **SIERRA** would be meeting with the firearms source to possibly purchase firearms to hold for UC-1. During this conversation, **SIERRA** also asked UC-1, if he/she wanted to purchase fentanyl or methamphetamine from the source. From October 31 to November 7, **SIERRA** sent UC-1 photos of several firearms, including a rifle, a shotgun, and a machine gun conversion device, as well as two bags of ammunition for various prices.

21. On November 8, 2023, I was present on surveillance, when UC-1 and UC-2, equipped with recording devices, met with **SIERRA** at **SUBJECT PREMISES 2** to purchase six firearms and one machine gun conversion device. On November 14, I later obtained records from Public Storage management showing that **SIERRA** is the lessee for **SUBJECT PREMISES 2.**

22. Based on my conversations with UC-1 and UC-2 and review of the recording device footage, I know that **SIERRA**

placed a cardboard box in the UCs' vehicle. Then the UCs directed **SIERRA** to place the long guns, which were wrapped in a blanket located on the orange cart, a Mavrick Arms Shotgun, model 88 bearing serial number MV51739F, and a Winchester Rifle, Model 70 CAL bearing serial number G2232694, in the trunk of the UCs' vehicle. While inside the UCs' vehicle, **SIERRA** removed a white plastic bag from the cardboard box. **SIERRA** gave UC-2 the white plastic bag, which contained eleven rounds of 19 caliber ammunition and nine rounds of assorted 12 caliber ammunition.

23. Based on my review of the recorded footage, I am also aware of the following:

a. **SIERRA** placed a pistol lock box on the center console of the UCs' vehicle and handed UC-2 the cardboard box. Inside the cardboard box were a Walther pistol Model PP bearing serial number 358038, and a machinegun conversion device. Inside the lock box was a Sig Sauer pistol Model P226 bearing serial number U 374 094, and a magazine loaded with ten rounds of 9 caliber ammunition. Additionally, **SIERRA** handed the UCs 0.98 gross grams of suspected methamphetamine as a free sample. **SIERRA** stated to the UCs that if the UCs wanted to purchase more methamphetamine from the source of the sample, they should inform **SIERRA** and he would facilitate the sale.

b. **SIERRA** then received a message on the cellular phone associated with the Subject Telephone, which he was holding in his hand. **SIERRA** told the UCs he was going to go pick up the other two firearms from the firearms source and then come back.

c. After **SIERRA** met with his source, **SIERRA** gave UC-2 a plastic bag. Contained inside the plastic bag were two firearms: A Smith & Wesson pistol Model SW40VE bearing serial number RBP3237, and a Smith & Wesson revolver Model 442 bearing serial number CXB1749. Additionally, the plastic bag contained twelve rounds of 40 caliber ammunition and ten rounds of 38 caliber ammunition.

d. **SIERRA** agreed to exchange phone numbers with UC-2. While still in the UCs' vehicle, UC-2 dictated his/her telephone number to **SIERRA**. **SIERRA** entered UC-2's telephone number into his device and placed a call. The number 310-978-7198 (i.e., the Subject Telephone) then appeared on UC-2's device.

24. I was informed by UC-2 that after the November 8, 2023 controlled firearms purchase, **SIERRA** was in constant contact with UC-2 via text message on the Subject Telephone. Throughout UC-2's communication with **SIERRA** on the Subject Telephone, **SIERRA** consistently offered UC-2 various types of firearms and provided photographs of those firearms for sale. **SIERRA** additionally provided UC-2 with information about **SIERRA**'s multiple firearm sources located outside of California.

E. Agents Review Surveillance Footage Capturing SIERRA At SUBJECT PREMISES 2 on Two of the Days of the Controlled Purchases

25. On or about December 18, 2023, law enforcement agents conducted surveillance of **SUBJECT PREMISES 2**. That same day, I reviewed surveillance footage from the Public Storage facility leading to **SUBJECT PREMISES 2** for the dates of September 28,

2023, and November 8, 2023. On both dates, **SIERRA** is seen driving **SUBJECT VEHICLE 1** towards the entry/exit gate of the Public Storage facility, and entering the gate. **SIERRA** then drives and parks **SUBJECT VEHICLE 1** in front of the entrance to building 1930 of the Public Storage facility. **SIERRA** is also captured on video exiting **SUBJECT VEHICLE 1**, entering a code to unlock the building door, and entering the building. Hallway cameras show **SIERRA** navigate the building and elevator toward his storage unit (identified as C231; i.e., **SUBJECT PREMISES 2**).

26. Specifically, according to surveillance footage, on September 28, when **SIERRA** reentered the elevator after going to **SUBJECT PREMISES 2**, there was a bulge in the right pocket of **SIERRA**'s pants that was not there previously.

27. Specifically, according to surveillance footage, on the date of November 8, 2023, **SIERRA** entered the elevator on the first floor with an orange moving cart. **SIERRA** exited the elevator with what appear to be firearms covered by a blanket on the orange moving cart. The firearms covered by a blanket on the orange moving cart were consistent with the firearms that were sold to UC-1 and UC-2 on November 8, 2023. Surveillance recordings also showed that **SIERRA** met with the individual believed to be **SIERRA**'s source of firearms in the front parking lot of the Public Storage facility two times during the controlled purchase on November 8, 2023. The firearms source was seen on surveillance recordings handing **SIERRA** firearms which

were consistent with the firearms that UC-1 and UC-2 later purchased from **SIERRA** that day.

F. On December 19, 2023, SIERRA Sells UC-2 One Firearm.

28. Based on my review of messages with UC-2 and SIERRA, between November 8 and December 19, 2023, UC-2 and **SIERRA** had consistent conversations about the sale of firearms via direct text message through the Subject Telephone. Specifically, On December 18, **SIERRA** sent a picture to UC-2 of a Ruger Pistol and informed UC-2 that the Ruger Pistol was for sale. On December 19, UC-2 confirmed with **SIERRA** that UC-2 was interested in purchasing the Ruger.

29. On December 19, 2023, UC-2 purchased a Ruger Pistol, model CCI bearing serial number 323-91154 from **SIERRA** at the location of 1622 E. Palm Ave in El Segundo, California. I have reviewed recording device footage, the reports from this event, and had a conversation with UC-1, and am aware of the following:

a. Prior to the UC arriving, surveillance units observed **SIERRA** leave from the direction of **SUBJECT PREMISES 1.**

b. During the controlled purchase, **SIERRA** handed UC-2 a Ruger Pistol model CCI bearing serial number 323-91154 in exchange for $1,000. SIERRA discussed with UC-2 that **SIERRA** is working with a Texas firearm source to transfer more firearms from Texas to Los Angeles.

c. After the controlled purchase, **SIERRA** exited the UC's vehicle and walked back in the direction of **SUBJECT PREMISES 1**, which is located less than a block away. Surveillance units observed SIERRA enter the apartment complex

of **SUBJECT PREMISES 1** and walk in the direction of **SUBJECT PREMISES 1**. Due to **SUBJECT PREMISES 1** being located at the far east corner of the apartment complex and all apartment unit doors facing inward to an interior courtyard not visible to the street, surveillance units did not have the ability to observe SIERRA walk directly into **SUBJECT PREMISES 1**.

G. SIERRA Does Not Have A License To Deal Firearms

30. ATF maintains a database of individuals that possess a federal firearms license ("FFL"). An FFL allows an individual to legally engage in the business of dealing firearms. On October 6, 2023, an ATF Industry Operations Investigator checked available internal ATF databases to determine whether **SIERRA** possessed an FFL. Based on my review of a report, **SIERRA** is not in the database as a current, former, or pending applicant or licensee.

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

31. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, and in their residences.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residence. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residence, including in the form of calendar entries and location data.

e. Drug traffickers often use vehicles to transport their narcotics and may keep stashes of narcotics in their

vehicles in the event of an unexpected opportunity to sell narcotics arises.

f. Drug traffickers often maintain on hand large amounts of United States currency in order to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence or in safes. They also often keep other items related to their drug trafficking activities at their residence, such as digital scales, packaging materials, and proceeds of drug trafficking. These items are often small enough to be easily hidden and thus may be kept at a drug trafficker's residence even if the drug trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

VI. TRAINING AND EXPERIENCE ON FIREARMS OFFENSES

32. From my training, personal experience, and the collective experiences related to me by other law enforcement

officers who conduct who conduct firearms investigations, I am aware of the following:

a. Persons who possess, purchase, or sell firearms generally maintain records of their firearm transactions as items of value and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such in their digital devices. It has been my experience that prohibited individuals who own firearms illegally will keep the contact information of the individual who is supplying firearms to prohibited individuals or other individuals involved in criminal activities for future purchases or referrals. Such information is also kept on digital devices.

b. Many people also keep mementos of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their digital devices. These photographs and recordings are often shared via social media, text messages, and over text messaging applications.

c. Those who illegally possess firearms often sell their firearms and purchase firearms. Correspondence between persons buying and selling firearms often occurs over phone calls, e-mail, text message, and social media message to and from smartphones, laptops, or other digital devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price. In my experience, individuals who engage in street sales of firearms frequently use phone calls, e-mail, and text messages to communicate with each other regarding firearms that the sell or offer for sale.

In addition, it is common for individuals engaging in the unlawful sale of firearms to have photographs of firearms they or other individuals working with them possess on their cellular phones and other digital devices as they frequently send these photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms.

d. Individuals engaged in the illegal purchase or sale of firearms and other contraband often use multiple digital devices.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[3]

33. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

d. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the

[3] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

e. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

f. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

g. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures

are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

34. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

35. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

36. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress **SIERRA**'s thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of **SIERRA**'s face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

37. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VIII. CONCLUSION

38. For all of the reasons described above, there is probable cause to believe that **SIERRA** has committed a violation of 21 U.S.C. § 841(a)(1), (b)(1)(B) (Distribution of a Controlled Substance). There is also probable cause that the items listed in Attachment B, which constitute evidence, fruits and instrumentalities of the Subject Offenses, will be found in a search of the SUBJECT PREMISES described in Attachment A-1 and A-2, the SUBJECT VEHICLES described in Attachment A-3 and A-4, and the person of **SIERRA** described in Attachment A-5.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 29th day of January, 2024.

THE HONORABLE CHARLES EICK
UNITED STATES MAGISTRATE JUDGE